

A partition of the hypercube into cosets of maximally nonparallel Hamming codes

Denis S. Krotov*

Abstract

By use of the Gold map, we construct a partition of the hypercube into cosets of Hamming codes that have minimal possible pairwise intersection cardinality.

Let $m \geq 3$ be odd and let F be the finite field $\text{GF}(2^m)$ of order 2^m . Let σ be a power of 2, and assume that $\sigma \pm 1$ and $2^m - 1$ are relatively prime (that is, both $x \rightarrow x^{\sigma+1}$ and $x \rightarrow x^{\sigma-1}$ are one-to-one mappings), which is, by simple arguments, equivalent to the condition $\gcd(s, m) = 1$, where $\sigma = 2^s$. For example, $\sigma = 2$. We will treat the codes C of length 2^m as collections of subsets of F , i.e., $C \subset 2^F$.

Recall some facts:

- (A) for all $x, y \in F$: $(x + y)^\sigma = x^\sigma + y^\sigma$ (derived from $(x + y)^2 = x^2 + y^2$);
- (B) for all $x \in F$: $x^\sigma + x + 1 \neq 0$ (indeed, otherwise $(x + 1)^{\sigma+1} = (x + 1)(x + 1)^\sigma = (x + 1)(x^\sigma + 1) = x^{\sigma+1} + x^\sigma + x + 1 = x^{\sigma+1}$, which is impossible as $f(x) = x^{\sigma+1}$ is one-to-one);
- (C) the cardinality of the code $B = \{X \in 2^F : \sum_{x \in X} 1 = 0, \sum_{x \in X} x = 0, \sum_{x \in X} x^{\sigma+1} = 0\}$ is $2^{2^m - 2m - 1}$ (in fact, B is a linear distance-6 code of maximal cardinality among the linear distance-6 codes of length 2^m [3]; in the case $\sigma = 2$, a BCH code).

For $\alpha \in F$, $p \in \{0, 1\}$, define the code H_α^p as the collection of subsets X of F satisfying

$$\begin{aligned} \sum_{x \in X} 1 &= p, \\ \sum_{x \in X} (x + \alpha)^{\sigma+1} &= 0. \end{aligned}$$

*Sobolev Institute of Mathematics, pr. Akademika Koptiyuga 4, Novosibirsk 630090, Russia. E-mail: krotov@math.nsc.ru

Theorem. (i) The codes H_α^1 , $\alpha \in F$, are mutually disjoint. (ii) Two different codes H_α^0 and H_β^0 have the intersection of cardinality 2^{2^m-2m} .

Proof. An element X of the intersection of H_α^p and H_β^p satisfies

$$\sum_{x+\alpha \in X} 1 = p \quad (1)$$

$$\sum_{x+\alpha \in X} x^{\sigma+1} = 0 \quad (2)$$

$$\sum_{x+\alpha \in X} (x + \alpha + \beta)^{\sigma+1} = 0 \quad (3)$$

We derive

$$\begin{aligned} \sum_{x+\alpha \in X} (x + \alpha + \beta)^{\sigma+1} &= \sum_{x+\alpha \in X} (x + (\alpha + \beta))^\sigma (x + (\alpha + \beta)) \\ &\stackrel{(A)}{=} \sum_{x+\alpha \in X} x^{\sigma+1} + \sum_{x+\alpha \in X} x^\sigma (\alpha + \beta) + \sum_{x+\alpha \in X} x (\alpha + \beta)^\sigma + \sum_{x+\alpha \in X} (\alpha + \beta)^\sigma \\ &\stackrel{(2)(A)(1)}{=} \left(\sum_{x+\alpha \in X} x \right)^\sigma (\alpha + \beta) + \left(\sum_{x+\alpha \in X} x \right) (\alpha + \beta)^\sigma + p (\alpha + \beta)^\sigma \end{aligned}$$

For $p = 1$ and $\alpha \neq \beta$, the last expression cannot be equal to 0, by (B), which contradicts (3) and proves (i).

For $p = 0$, it is equal to

$$\left(\sum_{x+\alpha \in X} x \right) \left(\left(\sum_{x+\alpha \in X} x \right)^{\sigma-1} + (\alpha + \beta)^{\sigma-1} \right) (\alpha + \beta),$$

which implies, together with (3) and $\alpha \neq \beta$, that

$$\text{either } \sum_{x+\alpha \in X} x = 0 \text{ or } \sum_{x+\alpha \in X} x = \alpha + \beta.$$

By (C), each of these two cases, together with (1) and (2), has exactly 2^{2^m-2m-1} solutions for X . So, there are 2^{2^m-2m} solutions in total, which proves (ii). \blacktriangle

As a **corollary**, we partitioned all the odd-cardinality subsets of F into 2^m cosets H_α^1 of extended Hamming codes such that every two different cosets are maximally nonparallel, that is, the corresponding extended Hamming codes have minimal possible intersections (in general, two extended Hamming codes can intersect in 2^{2^m-2m-1} elements, see e.g. (C), but in this case their odd cosets necessarily intersect).

Remark. We can consider α as the “color” of the elements of H_α^1 . It is easy to see that, given an odd-cardinality set $X \subset F$, its color can be calculated by the formula

$$\alpha = \alpha(X) = \sum_{x \in X} + \left(\sum_{x, y \in X, x \neq y} x^\sigma y \right)^{1/(\sigma+1)}.$$

By removing the zero element from all X , we obtain a partition of the $(2^m - 1)$ -cube into maximally nonparallel cosets of Hamming codes. The first ($n = 3$) partition from our series belongs to the classification of the partitions of the 7-cube into cosets of Hamming codes in [5].

Automorphisms and orbits. Let us consider some isometries of the space that stabilize the constructed partition $\{H_\alpha^1\}_{\alpha \in F}$ of the odd-cardinality subsets of F . For convenience, define $H_\alpha(\beta)$, $\alpha, \beta \in F$, as the set of odd-cardinality subsets $X \subset F$ satisfying

$$\sum_{x \in X} (x + \alpha)^{\sigma+1} = \beta^{\sigma+1}$$

(in particular, $H_\alpha(0) = H_\alpha^1$), and define H as the set of even-cardinality subsets $X \subset F$ satisfying

$$\sum_{x \in X} x = 0$$

(recall that H is an extended Hamming code; so, every odd-cardinality subset of F is at distance one from exactly one element of H).

Direct verification confirms the validity of the following four statements:

Lemma 1. *For every δ from F , the permutation $x \rightarrow x + \delta$ of F maps $H_\alpha(\beta)$ to $H_{\alpha+\delta}(\beta)$.*

Lemma 2. *For every μ from F , the permutation $x \rightarrow \mu x$ of F maps $H_\alpha(\beta)$ to $H_{\mu\alpha}(\mu\beta)$.*

Lemma 3. *The automorphism $x \rightarrow x^2$ of the field F maps $H_\alpha(\beta)$ to $H_{\alpha^2}(\beta^2)$.*

Lemma 4. *For every Y from H , the mapping $X \rightarrow X \triangle Y$ maps $H_\alpha(\beta)$ to $H_\alpha((\beta^{\sigma+1} + s_Y)^{1/(\sigma+1)})$ where $s_Y = \sum_{x \in Y} x^{\sigma+1}$. In particular, if $s_Y = 0$, it maps H_α^1 to itself.*

By an *automorphism* of the partition $\mathbf{H} = \{H_\alpha^1\}_{\alpha \in F}$ we mean an isometry of the space (i.e. a permutation of F and/or a translation $X \rightarrow X \triangle Y$ where Y is a fixed subset of F) that maps every cell of \mathbf{H} to another cell of \mathbf{H} . The partition is called *vertex-transitive* if the automorphism group acts transitively on the vertices, odd-cardinality subsets of F . That is, for every two odd-cardinality subsets X, Y of F there is an automorphism of \mathbf{H} that

sends X to Y . Similarly, the *cell transitivity* is defined, which property is, naturally, weaker than the vertex transitivity.

Lemma 1 shows that the constructed partition is cell-transitive (see [6] for other examples of cell-transitive partitions). Moreover, the odd-cardinality subsets of F are partitioned into at most two orbits under the action of the automorphism group of \mathbf{H} (indeed, by Lemmas 4 and 1, every vertex at distance 1 from $Y \in H$, $s_Y = 0$, can be sent to $\{0\}$ by an automorphism of \mathbf{H} ; by Lemmas 4, 2, and 1, every vertex at distance 1 from $Y \in H$, $s_Y \neq 0$, can be sent to $\{0\}$ by a space isometry that maps the cells of \mathbf{H} to the cells of $\mathbf{H}' = \{H_\alpha(1)\}_{\alpha \in F}$).

A computer experiment shows that for $m = 5, 7, 9, 11, 13$ the partition is not vertex-transitive (for $m = 3$, it is); i.e., the number of the orbits is exactly 2. An invariant that distinguishes the vertices of different orbits is the number of two-color squares in the neighborhood: for a given vertex X , we count the number Q_X of quadruples $\{X \triangle \{x, y\}, X \triangle \{y, z\}, X \triangle \{z, v\}, X \triangle \{v, x\}\}$ such that $\alpha(X \triangle \{x, y\}) = \alpha(X \triangle \{z, v\})$, and $\alpha(X \triangle \{y, z\}) = \alpha(X \triangle \{v, x\})$. For two vertices $X = \emptyset$ and Y from different orbits, the numbers Q_X and Q_Y are different. Moreover, they depend on σ , which implies that the construction, for fixed $m = 5, 7, 9, 11, 13, \dots(?)$, gives inequivalent partitions. Here is the listing of the calculated tuples $(2^m, \sigma + 1, Q_X, Q_Y)$:

$(2^5, 3, 155, 115)$	$(2^7, 3, 2667, 1995)$	$(2^{13}, 3, 8412157, 8385533)$
$(2^5, 5, 0, 120)$	$(2^7, 5, 2667, 1995)$	$(2^{13}, 5, 8518640, 8385520)$
$(2^{11}, 3, 540408, 523512)$	$(2^7, 9, 0, 2016)$	$(2^{13}, 9, 9157538, 8385442)$
$(2^{11}, 5, 585442, 523490)$	$(2^9, 3, 36792, 32184)$	$(2^{13}, 17, 7879742, 8385598)$
$(2^{11}, 9, 607959, 523479)$	$(2^9, 5, 18396, 32220)$	$(2^{13}, 33, 6388980, 8385780)$
$(2^{11}, 17, 360272, 523600)$	$(2^9, 17, 0, 32256)$	$(2^{13}, 65, 0, 8386560)$
$(2^{11}, 33, 0, 523776)$		

(it is sufficient to consider only the cases $\sigma < 2^{m/2}$, as the partitions for $\sigma = 2^s$ and for $\sigma = 2^{m-s}$ coincide, which easily follows from the identity $x^{2^s+1} = (x^{1+2^{m-s}})^{2^s}$).

Observations. 1. For $\sigma = 2^{(m-1)/2}$, we have got $Q_X = 0$.

2. The value Q_Y is rather close to the “average” value $D/(2^m - 1)$ where $D = (2^m - 1)(2^{m-1} - 1)2^{m-2}$ is the number of the pairs $\{X \triangle \{x, y\}, X \triangle \{z, v\}\}$ such that $\alpha(X \triangle \{x, y\}) = \alpha(X \triangle \{z, v\})$.

3. A two-color square have never been extended to a three-color octahedron; i.e., $\alpha(X \triangle \{x, z\}) \neq \alpha(X \triangle \{y, v\})$, in the notations above.

4. The length- 2^7 partitions with $\sigma + 1 = 3$ and $\sigma + 1 = 5$ are nonequivalent (while (Q_X, Q_Y) coincide).

A natural **conjecture** is that the number of orbits is 2 for every odd $m \geq 5$. If it is true, then every automorphism of \mathbf{H} is a composition of automorphisms from Lemmas 1, 2, 3, and 4 (with $s_Y = 0$). For $\sigma = 2$, this follows from [2] (any automorphism of \mathbf{H} is an automorphism of the

code $\{Y \in H : s_Y = 0\}$, which is an extended double-error-correcting BCH code).

Questions and remarks. 1. As follows from the proof, the claim (i) of the theorem will remain valid if we replace the function $f(x) = x^{\sigma+1}$ by an arbitrary permutation (bijective function) $f : F \rightarrow F$ such that for all $\alpha \neq 0$ the set $H_\alpha = \{f(x) + f(x + \alpha) : x \in F\}$ is an affine subspace (over $\text{GF}(2)$) of F (the sum of odd number of elements of H_α belongs to H_α , which does not contain 0 as f is bijective). A class of functions that obviously satisfy this condition is the class of quadratic function, i.e., the vector functions whose components are represented as polynomials of degree at most 2. For such permutations, the cardinalities of the mutual intersections of the corresponding Hamming codes can be counted in terms of the cardinalities of H_α , using the technique from the second part of the theorem. Another appropriate class of permutations is the following. A permutations $f : F \rightarrow F$ is called *crooked* [1] if for all $\alpha \neq 0$ the set H_α is an affine hyperplane. The Gold function is crooked. At the moment, all known crooked functions are quadratic. Does (ii) hold for the non-quadratic crooked permutations $f(x)$ (if there are some)? See [8] for other applications of the crooked permutations in construction of different extremal combinatorial structures.

2. Are there exist such partitions for even m ? In [4], partitions of the space into mutually nonparallel cosets of Hamming codes are constructed for all $m \geq 3$. The problem of minimizing mutual intersection of the Hamming codes for such a partition remains open for even m .

Acknowledgment. The author thanks Sergey Avgustinovich for discussions and Gohar Kyureghyan for consulting in the area of crooked functions.

References

- [1] T. D. Bending and D. Fon-Der-Flaass. Crooked functions, bent functions, and distance regular graphs. *Electr. J. Comb.*, 5:R34(1–14), 1998.
- [2] T. P. Berger. The automorphism group of double-error-correcting BCH codes. *IEEE Trans. Inf. Theory*, 40(2):538–542, 1994. DOI: 10.1109/18.312182.
- [3] C. Carlet, P. Charpin, and V. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Des. Codes Cryptography*, 15(2):125–156, 1998. DOI: 10.1023/A:1008344232130.

- [4] O. Heden and F. I. Solov'eva. Partitions of F^n into non-parallel Hamming codes. *Adv. Math. Commun.*, 3(4):385–397, 2009. DOI: 10.3934/amc.2009.3.385.
- [5] K. T. Phelps. An enumeration of 1-perfect binary codes. *Australas. J. Comb.*, 21:287–298, 2000.
- [6] F. I. Solov'eva. On transitive partitions of an n -cube into codes. *Probl. Inf. Transm.*, 41(1):23–31, 2009. DOI: 10.1134/S0032946009010037.
- [7] F. I. Solov'eva and G. K. Gus'kov. On construction of vertex-transitive partitions of the n -cube into perfect codes. *Discrete Math. Appl.*, 5(2):301–311, 2011. DOI: 10.1134/S1990478911020189.
- [8] E. R. van Dam and D. Fon-Der-Flaass. Codes, graphs, and schemes from nonlinear functions. *Eur. J. Comb.*, 24(1):85–98, 2003. DOI: 10.1016/S0195-6698(02)00116-6.